

REMARKS

Claims 1-3, 5, 9-13, 18, 21-23 and 25-27 are pending. By this Amendment, claims 1, 3, 5, 10, 13, 22 and 25 are amended. No new matter is added.

Claims 1, 10, 22 and 25 are amended to place the claims in condition for allowance. Claims 3, 5 and 13 are amended to improve form. Support for the claims is found in the disclosure as originally filed.

With respect to claims 1, 10, 22 and 25, it is submitted that the additional feature of “the key schedule unit provides the round key to the block round unit for each round without storing expanded keys being generated by the key schedule unit” was previously deleted by an amendment filed on November 17, 2008, but the feature would have placed the claims in condition for allowance. With respect to claim 25, it is noted that the added feature is a similar feature in varying scope.

During the September 11, 2009 in-person interview, it was briefly discussed whether the addition of the previously deleted feature would place the claims in condition for allowance, and the Examiner tentatively indicated that the addition would place the claims in condition for allowance.

For the following reasons, reconsideration is respectfully requested.

Claim rejections – 35 U.S.C. § 103

Claims 1, 2, 5, 9-11, 18 and 21-23 are rejected under 35 U.S.C. § 103(a) over Wasilewski (U.S. Patent No. 5,420,866), in view of Daemen (“AES Proposal: Rijndael”), and in further view of Adler (U.S. Patent No. 4,255,811).

Claims 3, 12 and 13 are rejected under 35 U.S.C. § 103(a) over Wasilewski, in view of Daemen, in view of Adler, and in further view of Mroczkowski (“Implementation of the Block cipher Rijndael using Altera FPGA”).

Claims 25-27 are rejected under 35 U.S.C. § 103(a) over Wasilewski, in view of Daemen, and in further view of Vanstone (U.S. Patent No. 6,212,281).

The rejections are respectfully traversed.

As amended, it is respectfully submitted that Wasilewski, Daemen and Adler, either individually or in combination, fail to disclose or suggest each and every feature of claim 1, namely, an apparatus for encrypting/decrypting a real-time input stream comprising a processor configured to receive a data stream of bytes wherein the data stream is an MPEG data stream or a Digital Satellite Service (DSS) data stream, convert the data stream into data blocks, provide the data blocks for encryption or decryption, receive encrypted or decrypted data blocks, convert the received encrypted or decrypted data blocks into bytes, and output the bytes, wherein the processor generates a start key signal when a new round key is needed for every round; a key schedule unit configured to provide a round key for every round in accordance with the start key signal and an input key having a variable size to provide the round key for the encryption or decryption for each round, wherein the input key size is one of 128, 192, and 256 bits; and a block round unit configured to receive converted data blocks from the processor, receive the round key from the key schedule unit, encrypt or decrypt the received data blocks, and provide the encrypted or decrypted data blocks to the processor, wherein the key schedule unit selects a 128 bit round key to the block round unit for each round using a key register having a capacity of $\{(size\ of\ an\ inputted\ block) * (size\ of\ one\ round)\}$, and the key schedule unit provides the round key to the block round unit for each round without storing expanded keys being generated by the key schedule unit.

Additionally, as amended, it is respectfully submitted that Wasilewski, Daemen and Adler, either individually or in combination, fail to disclose or suggest each and every feature of claims 10 and 22, which recite similar features of varying scope.

Further, as amended, it is respectfully submitted that Wasilewski, Daemen and Vanstone fail to disclose or suggest each and every feature of claim 25, which recites similar features of varying scope.

Thus, it is respectfully submitted that claims 1, 10, 22 and 25 are patentably distinguishable over the applied references and their combination. Claims 2, 5 and 9, which depend from claim 1; claims 11, 18 and 21, which depend from claim 10; claim 23, which depends from claim 22; and claims 26 and 27, which depend from claim 25, are likewise patentably distinguishable over the applied references and their combination for at least the reasons discussed above and/or for the additional features they recite.

Further, it is respectfully submitted the additional rejections noted in the Office Action have also been overcome as the claims rejected therein are dependent claims and additionally applied references also do not teach or suggest the features recited in the corresponding independent claims.

Withdrawal of the rejections is respectfully requested.

CONCLUSION

In view of the above amendment and/or remarks, Applicant believes the pending application is in condition for allowance.

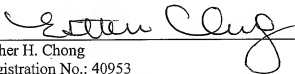
Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Seth S. Kim, Reg. No. 54,577, at the telephone number of the undersigned below to conduct an interview in an effort to expedite prosecution in connection with the present application.

If necessary, the Director is hereby authorized in this, concurrent, and future replies to charge any fees required during the pendency of the above-identified application or credit any overpayment to Deposit Account No. 02-2448.

Dated: MAR 30 2010

Respectfully submitted,

By


Esther H. Chong

Registration No.: 40953

BIRCH, STEWART, KOLASCH & BIRCH, LLP

8110 Gatehouse Road, Suite 100 East

P.O. Box 747

Falls Church, VA 22040-0747

703-205-8000